Apr 18

REMINDERS

(•) HW 6 due by 11:59pm on Wed

(•) Video due by 11:59pm in ~ 3.5 weeks (Wed, May 11)

RECAP

(•) Explicit codes that can be decoded up to $\frac{1}{2} \cdot$ (Zyablov bound) (*)

(•) Explicit BSC_p capacity achieving codes (*)

(*) Assuming exists poly time unique decoding of RS codes (upto $\frac{1-R}{2}$ frac of errors in $O(N^3)$ ops)

TODAY

(•) Proof readers : Ashley, Yaswanth, Prashanth

(•) Unique decoder for RS codes [Welch-Berlekamp algo]

Last missing piece: Unique decoder for RS codes.

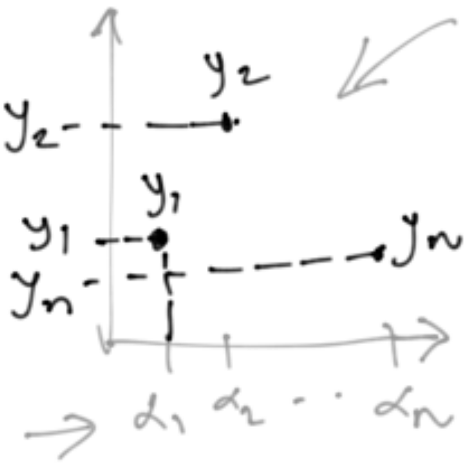
Given $1 \le k \le n$, $[n, k, d = n-k+1]_q$ RS code. Fix eval pts $\underbrace{\alpha_1, \ldots, \alpha_n}_{\text{distinct} \Rightarrow q \geq n} \in \mathbb{F}_q$

(·) rcvd word $\bar{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$

Syntactic switch: $\quad \uparrow \alpha_1 \qquad \uparrow \alpha_n$

$\equiv (\alpha_1, y_1), \ldots, (\alpha_i, y_i), \ldots, (\alpha_n, y_n) \in \mathbb{F}_q \times \mathbb{F}_q$

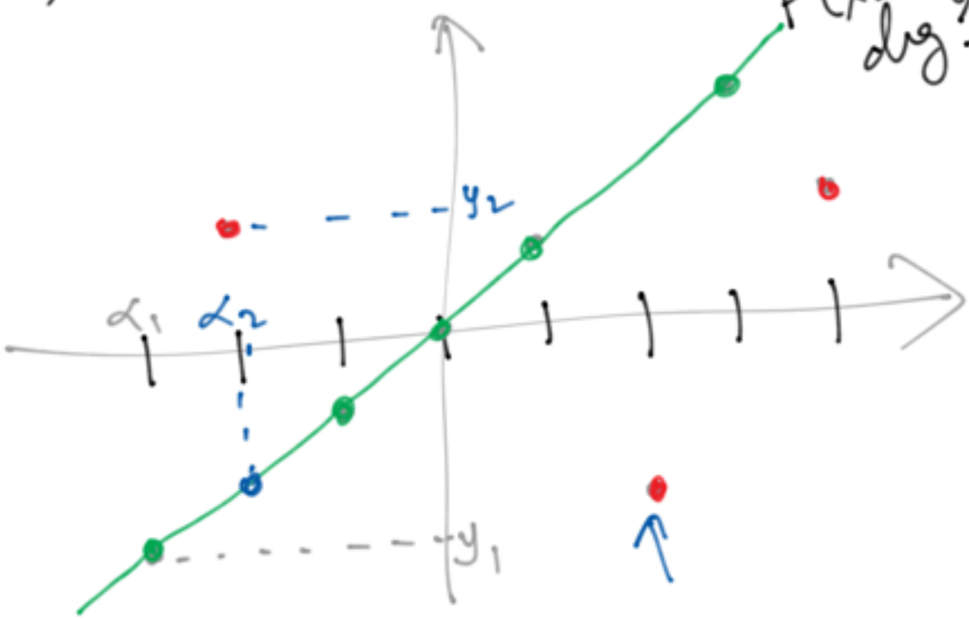
set → Hashes for fingerprints



output/want: poly $P(X)$ of deg $\le k-1$ s.t for at least $n-e$ values of $i \in [n]$, $P(\alpha_i) = y_i$ $\equiv$ $\le e$ values of $i \in [n]$, $P(\alpha_i) \neq y_i$ $\Rightarrow$ $P(X)$ is unique

$\equiv \Delta\left(\bar{y}, \left(P(\alpha_i)\right)_{i=1}^{n}\right) \le e$

$e < \dfrac{n-k+1}{2} \Rightarrow$ frac of error $\le \dfrac{1-R}{2}$



$n = 8$

$k = 2$

$e < \dfrac{n-k+1}{2}$

$= \dfrac{8-2+1}{2}$

$e = 3$

Welch-Berlekamp (thought process)

(Gemmell-Sudan)

1. Assume you know $P(x)$ (obviously also know $\bar{y}$)
2. Derive some polynomial identities involving $P(x)$ & $\bar{y}$
3. ______ linear equations s.t. $P(x)$ is a valid solution to these equations
   ($\Rightarrow$ "forget" that you knew $P(x)$)
4. Solve that equation (Gaussian Elimination)
   Q2 on HW 0
4.1 Argue that $P(x)$ is the only solutions.

Let $P(x)$ be s.t. $\deg(P) < k$ & $P(\alpha_i) \neq y_i$ for $\leq e$ locations $i \in [n]$

Error locator poly: $E(x)$ s.t.

$\forall i \quad P(\alpha_i) \neq y_i \ , \quad E(\alpha_i) = 0 \Rightarrow$ the roots of E are the locations of errors

$$E(x) = \prod_{i : P(\alpha_i) \neq y_i} (X - \alpha_i)$$

monic

Claim: $\forall i \in [n] \quad y_i E(\alpha_i) = P(\alpha_i) \cdot E(\alpha_i)$

Pf: case 1: $P(\alpha_i) = y_i$

Case 2: $P(\alpha_i) \neq y_i$

Claim: $\forall i \in [n]$ $\boxed{y_i E(\alpha_i) = P(\alpha_i) \cdot E(\alpha_i)}$

$\rightarrow$ Think of the coefficients of $P(X)$ $\leftarrow k$

& $E(X)$ as variables

$\uparrow$ deg $\le e$, + monic $\Rightarrow e$ vars

n equations in $k+e$ variables

$k+e \le k + \frac{n-k+1}{2} = \frac{n+k+1}{2} \le \frac{2n+1}{2} = n + \frac{1}{2}$

$\Rightarrow$ # variables $\le n$

n equations in n variables.

$\uparrow$ not linear equations

quadratic

Trick (linearization): replace product of two variables with a new variable.

Define $N(X) = P(X) \cdot E(X)$

$\deg(N) \le k-1+e = k+e-1$

$\forall i \in [n]$, $y_i E(\alpha_i) = N(\alpha_i)$

$\rightarrow$ n equations (linear)

$\rightarrow$ variables: coeffs of $E(X)$ & $N(X)$

$\Rightarrow$ #vars $= e + k+e = k+2e$

vars $\leq$ # eqns

$k+2e \leq n$ or $e \leq \frac{n-k}{2}$

this is fine since $e < \frac{n-k+1}{2}$

$\Rightarrow$ Solve this system of linear equations & get $E(X)$ and $N(X)$

from this can compute (hopefully) $P(X) \leftarrow \frac{N(X)}{E(X)}$

Welch-Berlekamp algo

<u>i/p:</u> $1 \leq k \leq n$, $0 < e < \frac{n-k+1}{2}$, n pairs $(\alpha_i, y_i) \in \mathbb{F}_q^2$

<u>o/p:</u> a poly $P(X)$ of deg $\leq k-1$ or FAIL

1. Compute a monic $E(X)$ of deg e & $N(X)$ of deg $\leq k+e-1$ s.t. $\forall i \in [n]$ $N(\alpha_i) = y_i \cdot E(\alpha_i)$
2. ~~If~~ no such E or N $\exists$, output FAIL
3. If $E(X)$ doesn't divide $N(X)$, output FAIL
4. $P(X) \leftarrow N(X)/E(X)$
5. If $\deg(P) \geq k$ or $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^{n}) > e$ output FAIL
6. Return $P(X)$